Kövér László
az Országgyűlés elnöke részére
Budapest

Iktatószám: .....

Tisztelt Elnök Úr!

Az egyes házszabályi rendelkezésekről szóló 10/2014. (II. 24.) OGY határozat (a továbbiakban: HHSZ) 137/A. § (1) bekezdése alapján iromány-nyilvántartásba vétel céljából megküldöm a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvényjavaslatnak (T/3314. szám) a HHSZ 46. § (10) bekezdése alapján megszerkesztett egységes javaslattervezetéhez készített indokolást.

Budapest, 2023. május „4.”

Tisztelettel:

Dömötör Csaba

Előterjesztői indokolás
a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló
2023. évi ... törvényhez

Általános indokolás

Ez az indokolás a jogalkotásról szóló 2010. évi CXXX. törvény 18. § (3) bekezdése, valamint a Magyar Közlöny kiadásáról, valamint a jogszabály kihirdetése során történő és a közjogi szervezetszabályozó eszköz közzététele során történő megjelöléséről szóló 5/2019. (III. 13.) IM rendelet 20. § (2) bekezdés a) pontja alapján a Magyar Közlöny mellékleteként megjelenő Indokolások Tárában közzétételre kerül.

Az Európai Unió által kidolgozott kiberbiztonsági tanúsítási rendszer hazai elemeként 2022. január 1-jétől a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) módosításának eredményeként a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH), valamint – a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében – a Kormány által kijelölt hatóság került kijelölésre a nemzeti kiberbiztonsági tanúsító hatósági feladatok elvégzésére. A 2021. évi törvénymódosítás az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és a tanácsi rendeletben (a továbbiakban: Rendelet) foglalt határidő betartását szolgálta, a kiberbiztonság érdemi újraszabályozására nem tett kísérletet.

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvényjavaslat (a továbbiakban: törvényjavaslat) két fő tárgykört fed le:

- kialakítja a kiberbiztonsági tanúsítás hazai keretrendszerét és emellett biztosítja a Rendelet érvényesülését, és

- a gazdasági élet jelentős ágazatainak szereplői számára kiberbiztonsági követelményeket határoz meg és hatósági felügyeleti rendszert vezet be.

A nemzeti kiberbiztonsági tanúsítási keretrendszer azt biztosítja, hogy a digitalizációs transzformáció eredményeként egyre szélesebb körben használt infokommunikációs termékek és szolgáltatások típusai, illetve fajtái tekintetében a tanúsító hatóság kiberbiztonsági elvárásokat, követelményeket fogalmazzon meg, rögzített módszertan szerint ezen követelmények, elvárások teljesülését értékelje, vizsgálja, valamint a kiberbiztonsági szempontoknak megfelelő termékek piaci felhasználását elősegítse.

A törvényjavaslat biztosítja, hogy az Európai Unió tanúsítási rendszere által le nem fedett infokommunikációs termékek és szolgáltatások esetében hazai tanúsítási követelmények kerüljenek meghatározásra.

A kiberbiztonsági követelményeket a termék gyártójának vagy a szolgáltatás nyújtójának kell teljesítenie. A követelményeknek való megfelelést olyan akkreditált megfelelőségértékelő szervezetek vizsgálják, amelyeket a tanúsító hatóság nyilvántartásba vett és – a törvényjavaslatban meghatározott esetekben – e tevékenységüket engedélyezte.

A törvényjavaslat felhatalmazást ad az SZTFH elnöke, valamint a hadiipar esetében a Kormány számára rendeletalkotásra, amelyben termékkategóriánként meghatározza az ún. tanúsítási sémákat, keretrendszereket (elvárásokat, követelményeket és értékelési módszertanokat).

A törvényjavaslat értelmében az SZTFH feladata a nemzeti kiberbiztonsági tanúsítási rendszerek kidolgozásával kapcsolatosan nyomon követni az európai kiberbiztonsági tanúsítási rendszerek fejlesztését, figyelemmel kísérni a kapcsolódó szabványosítási folyamatokat és értékelni a hatályos nemzeti kiberbiztonsági tanúsítási rendszereket.

Az SZTFH feladata továbbá információkat gyűjteni azon ágazatokról és szakterületekről, amelyek nem esnek európai kiberbiztonsági tanúsítási rendszer hatálya alá és ahol a kiberbiztonság növelése szükséges.

A törvényjavaslat által megteremteni hivatott egységes, az EU szabályoknak is megfelelő tanúsítási rendszer hozzájárul a hazai infokommunikációs-szektor teljesítményének és versenyképességének növeléséhez. A tanúsítványok kötelezővé tétele emeli az érintett termékek, illetve szolgáltatások minőségét és megbízhatóságát, nemzetközi szinten is versenyképesebbé, versenyállóbbá téve ezáltal a magyar gyártású termékeket, amely akár új piacok megnyitását is lehetővé teszi.

A törvényjavaslat III. Fejezete azokra a vállalatokra, szervezetekre fogalmaz meg kiberbiztonsági követelményeket, amelyek a társadalom és a gazdaság szempontjából alapvető igényeket elégítenek ki, úgymint energia, szállítás, egészségügy (beleértve a gyógyszergyárakat is), ivóvíz-szolgáltatók, egyéb közműszolgáltatók. A törvényjavaslat a digitális infrastruktúraszolgáltatókra is érvényes, ezek közé tartoznak a DNS-szolgáltatók, domainnév-regisztrátorok, felhőszolgáltatók, adatközpontok, elektronikus kommunikációs szolgáltatók, közcélú kommunikációs hálózatok.

A szabályozás emellett kiterjed olyan fontos vállalatokra is, amelyek a következő szektorokban tevékenykednek: postai és futárszolgáltatások, hulladékgazdálkodás, vegyipar, élelmiszergyártás, orvosi eszközök gyártása, számítástechnikai eszközök gyártása, nehézgépek gyártása, autóipar, online piacterek, online keresők.

A törvényjavaslat bevezeti a kiberbiztonsági kockázatelemzés követelményét, az elektronikus információs rendszerek biztonsági osztályba sorolásának és az egyes osztályokhoz tartozó biztonsági kontrollok implementálásának kötelezettségét. Rendelkezéseket tartalmaz továbbá a beszállítói (ellátási) lánc kiberbiztonsági kockázatainak csökkentésére, a biztonsági események Ibtv. szerinti eseménykezelő központ részére felé történő jelentésére.

A fenti követelmények megvalósulásának ellenőrzésére a törvényjavaslat felügyeleti jogkörrel ruházza fel az SZTFH-t, és rögzíti az ellenőrzés, nyilvántartás és bírságolás rendjét.

Részletes indokolás

1-2. §

A törvényjavaslat az alapvető fogalmakra vonatkozó értelmező rendelkezéseket és az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény rendelkezéseinek alkalmazására vonatkozó rendelkezéseket állapítja meg.

3-4. §

A törvényjavaslat tanúsítási rendszerekre vonatkozó rendelkezéseit az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat tanúsításával kapcsolatos hatósági tevékenységre kell alkalmazni. A

törvényjavaslat az általános rendelkezések között kizárja a megfelelőségértékelő szervezetek tevékenységéről szóló törvény rendelkezéseinek alkalmazását.

A törvényjavaslat a kiberbiztonsági tanúsítással kapcsolatos hatósági feladatok elvégzésére az SZTFH-t jelöli ki, valamint rögzíti, hogy a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány jelöli ki a tanúsító hatóságot.

5. §

A törvényjavaslat rögzíti a tanúsító hatóság alapvető feladatait a tanúsítási rendszerek nyomon követésével, fenntartásával és fejlesztésével, illetve az európai uniós képviselettel kapcsolatosan. Garanciális szabályként rögzítésre kerül az európai kiberbiztonsági tanúsítási rendszerek elsőbbsége, azaz nemzeti tanúsítási rendszer csak azon IKT-termékek, IKT-szolgáltatások és IKT-folyamatok esetében alkotható meg, amelyekre vonatkozóan nincs hatályos európai kiberbiztonsági tanúsítási rendszer. Ellenkező esetben a nemzeti tanúsítási rendszert a hatóság köteles hatályon kívül helyezni.

6-7. §

A törvényjavaslat a kiberbiztonsági tanúsítási rendszerekkel szemben alapvető követelményeket állapít meg. Rögzítésre kerülnek a nemzeti tanúsítási rendszerek biztonsági céljai, valamint azok tartalmi összetevői.

8. §

A törvényjavaslat rögzíti a nemzeti kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjeit, azaz arra vonatkozóan szolgál biztosítékkal, hogy az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok teljesítik a vonatkozó biztonsági követelményeket, biztonsági funkciókat és olyan szintű értékelésen estek át, amely az adott szinteknek megfelelő súlyú kiberbiztonsági fenyegetések, támadások kockázatainak minimalizálására törekszik. Az IKT-termékekre, az IKT-szolgáltatásokra és az IKT-folyamatokra az „alap", a „jelentős" és a „magas" megbízhatósági szintek közül egy vagy több szint határozható meg.

9. §

Figyelemmel arra, hogy nemzeti kiberbiztonsági tanúsítási rendszer alapján a megfelelőségértékelő szervezet bocsátja ki a nemzeti kiberbiztonsági tanúsítványt, illetve a gyártó a megfelelőségi nyilatkozatot, ezért a tanúsítvánnyal, illetve nyilatkozattal szembeni elvárások törvényi szinten kerülnek rögzítésre.

10. §

A törvényjavaslat rögzíti, hogy tanúsított vagy megfelelőségi nyilatkozattal rendelkező IKT-terméken, IKT-szolgáltatáson vagy IKT-folyamatban a tanúsítottság tényének jelzésére megfelelőségi jelölést kell elhelyezni, illetve tiltja olyan jelölés elhelyezését, amely hasonlít a megfelelőségi jelölés formájára, vagy azt a látszatot kelti, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat tanúsított, és így harmadik felet megtéveszthet.

11-12. §

A törvényjavaslat rögzíti a megfelelőségértékelő szervezettel, illetve a megfelelőségi önértékelést végző gyártóval kapcsolatos rendelkezéseket. Megfelelőségértékelő szervezetek esetében alapvető követelmény, hogy a szervezetet a nemzeti akkreditálásról szóló törvény szerint kijelölt akkreditáló

szerv akkreditálja vagy elismerje a külföldi akkreditált státuszát, valamint a tanúsító hatóság által történő nyilvántartásba vétel.

Megfelelőségi önértékelésre csak abban az esetben kerülhet sor, ha a nemzeti tanúsítási rendszer azt kifejezetten tartalmazza „alap" megbízhatósági szintnek megfelelő, alacsony kockázatot jelentő IKT-termékek, IKT-szolgáltatások és IKT-folyamatok esetében. Ebben az esetben a gyártónak nyilatkoznia kell arról, hogy a tanúsítási rendszerben foglalt követelmények vizsgálata megtörtént a tanúsítási rendszerben foglalt értékelési módszertan szerint. További követelmény, hogy a hatóság számára az előírt határidőn belül be kell nyújtani a szükséges dokumentációkat.

13. §

A törvényjavaslat meghatározza a tanúsító hatóság eljárására vonatkozó alapvető szabályokat. Európai tanúsítási rendszer esetében további követelményként rögzítésre került, hogy az Európai Bizottság számára meghatározott határidőn belül be kell jelenteni az akkreditált megfelelőségértékelő szervezeteket.

A törvényjavaslat rögzíti továbbá, hogy a tanúsító hatóság engedélyezési eljárást folytat le abban az esetben, ha egy európai tanúsítási rendszer konkrét vagy kiegészítő követelményeket vagy „magas" megbízhatósági szintet ír elő a rendszer keretében kiadandó kiberbiztonsági tanúsítványra és a tanúsító hatóság az ilyen tanúsítvány kiállításának feladatát egyes európai kiberbiztonsági tanúsítványok vonatkozásában vagy általános jelleggel átruházza megfelelőségértékelő szervezetre. Magas megbízhatósági szint esetében az engedély feltétele, hogy a megfelelőségértékelő szervezet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény alapján sérülékenységvizsgálatra feljogosított gazdálkodó szervezet legyen.

14. §

A törvényjavaslat rögzíti azokat az adatokat, amelyeket a tanúsító hatóság az általa vezetett nyilvántartásban kezel, amely nyilvántartás meghatározott adatfajták esetben közhiteles nyilvántartásnak minősül. Az adatok kezelésének célja az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságával összefüggő információk naprakészen tartása, valamint az azokat érintő sebezhetőséggel vagy rendellenességgel kapcsolatos feladatok, továbbá a tanúsító hatóság ellenőrzési és felügyeleti hatósági feladatainak ellátása. A törvényjavaslat rögzíti továbbá, hogy mely szervezetek számára lehet a nyilvántartásból adatot továbbítani, valamint kötelezi a megfelelőségértékelő szervezeteket az adatok változásairól történő adatszolgáltatásra.

15. §

A törvényjavaslat rögzíti a megfelelőségértékelő szervezettel, illetve a gyártóval szemben érvényesíthető szankciókat arra az esetre, ha a vonatkozó európai uniós vagy magyar jogszabályokban foglalt követelményeket és a kapcsolódó eljárási szabályokat nem teljesítik vagy nem tartják be. A tanúsító hatóság figyelmeztetést, valamint – ha a figyelmeztetés ellenére a szervezet a jogszabályban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti – az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nemteljesítés esetén megismételhető.

16. §

A törvényjavaslat rögzíti a tanúsító hatóság általános adatkezelésére vonatkozó szabályokat, egyúttal jogosultságot biztosít a tanúsító hatóságnak arra, hogy a hatósági feladatok ellátásához minősített adatot, személyes adatot vagy különleges adatot, üzleti titoknak, banktitoknak, fizetési

titoknak, biztosítási titoknak, értékpapírtitoknak, pénztártitoknak, orvosi titoknak és más hivatás gyakorlásához kötött titoknak minősülő adatot és törvény által védett egyéb adatot kizárólag a feladat ellátásának időtartama alatt, a célhoz kötöttség elvének figyelembevételével kezeljen. Megállapítja az adatkezelés maximális időtartamát, amelyet követően az adatokat a tanúsító hatóság információs rendszereiből és adathordozóiról törölni kell.

17-18. §, 1-2. melléklet

A kiberbiztonsági felügyeleti rendelkezéseket a törvényjavaslat 1. és 2. mellékletében felsorolt szervezetek (a továbbiakban: érintett szervezetek) elektronikus információs rendszerei tekintetében kell alkalmazni.

A törvényjavaslat kizárja a mikro- és kisvállalkozásokat az érintett szervezetek köréből az egyes – kiberbiztonsági szempontból kiemelt fontosságú – tevékenységeket folytató vállalkozások kivételével. A törvényjavaslat emellett kizárja az alkalmazási körből azokat az elektronikus információs rendszereket, amelyek az Ibtv. szerint az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeknek a létfontosságú tevékenységben működnek közre, továbbá azokat a programozható rendszereket, amelyek az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló kormányrendelet alá tartoznak.

19-20. §

A törvényjavaslat megállapítja azokat az alapvető követelményeket, amelyek az elektronikus információs rendszer, illetve az azon kezelt adatok bizalmasságához, sértetlenségéhez és rendelkezésre állásához nélkülözhetetlenek. Az alapvető követelményeket az elektronikus információs rendszer üzemeltetésében, karbantartásában vagy javításában közreműködőknek is be kell tartaniuk a szerződéses viszonyaikban. Rögzítésre kerülnek továbbá az érintett szervezet vezetőjének főbb feladatai és felelősségi köre.

Az érintett szervezet köteles az elektronikus információs rendszereket és az azon tárolt, továbbított vagy feldolgozott adatokat biztonsági osztályba sorolni és az egyes biztonsági osztályokhoz a külön jogszabályban meghatározott védelmi intézkedéseket alkalmazni. Ezek a védelmi intézkedések kiválthatóak tanúsított IKT termékkel, -szolgáltatással vagy -folyamattal.

21. §

A törvényjavaslat kötelezi a legfelső szintű domainnév-nyilvántartót központi adatbázis létrehozására, a domainnév-nyilvántartás kötelező adattartalmának meghatározása mellett. A kezelt adatok valódiságának fenntartása érdekében szabályozási kötelezettséget rögzít, továbbá közzétételi követelményt állapít meg a személyes adatnak nem minősülő adatok vonatkozásában. A törvényjavaslat rögzíti, hogy a legfelső szintű domainnév-nyilvántartó által kezelt adatok kezelésének célja a domainnevet kezelő adminisztratív kapcsolattartó, valamint a domainnév-használó természetes vagy jogi személy azonosíthatósága, valamint a kapcsolattartási adatok naprakészen tartása.

22. §

A törvényjavaslat alapján a kiberbiztonsági felügyeleti feladatok elvégzésére az SZTFH kerül kijelölésre. A felügyelet keretében a hatóság ellenőrzi a kiberbiztonsági követelmények betartását helyszíni ellenőrzés, rendkívüli ellenőrzés lefolytatásával vagy rendkívüli audit elrendelésével.

A kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény alapján mikro- és kisvállalkozás kategóriát meghaladó, kiemelten kockázatos szektorokban működő (1. melléklet szerinti) szervezetek, valamint a digitális infrastruktúra fenntartásával és működésével kapcsolatos tevékenységet végző szervezetek esetében a hatóság rendszeres, az SZTFH elnökének rendelete szerint elkészített éves ellenőrzési terv alapján végzi a kötelezettségek betartásának ellenőrzését. Az egyéb szervezetek esetében az audit eredmények, illetve a bejelentett biztonsági események adatai alapján, a kockázatok mérlegelését követően, azzal arányosan hajtja végre az ellenőrzéseket.

A törvényjavaslat felsorolja továbbá azokat az adatokat és dokumentumokat, amelyeket a hatóság jogosult az érintett szervezettől bekérni és megismerni.

23. §

A hatósági felügyeletet nem érintve, az érintett szervezet köteles kétévente auditot végeztetni arra felhatalmazott, független auditor által. Az audit végrehajtásának a célja az, hogy az érintett szervezet képes legyen felismerni az elektronikus információs rendszereit érintő kockázatokat, valamint a biztonsági követelményeknek való nemmegfelelés eseteit.

A törvényjavaslat rögzíti az audit végrehajtásának főbb szabályait, az auditorral kapcsolatos elvárások, továbbá az audit maximális díjának meghatározására az SZTFH elnökének rendeletében kerül sor.

A követelményeknek megfelelő és az audit végrehajtására jogosult gazdálkodó szervezetekről az SZTFH nyilvántartást vezet és az auditorokat hatósági hatáskörében ellenőrzi. Az audit végrehajtásáról, annak befejezését követően az auditor a hatóságot is tájékoztatja. Rögzítésre kerülnek továbbá a hatóság azonnali tájékoztatására vonatkozó kötelezettség esetkörei, továbbá az auditor adatkezelésére vonatkozó szabályok.

24. §

A törvényjavaslat a kiberbiztonsági követelmények be nem tartásával összefüggésben a hatóság számára szankcionálási lehetőségeket rögzít, amelyeket a hatóság a jogsértéssel arányos módon alkalmazhat. A hatóságnak lehetősége van bírság kiszabására is, amely nemteljesítés esetén megismételhető.

A közbiztonság és a közérdek védelme, valamint az állampolgárok preventív védelme okán a hatóság elrendelheti az érintett szervezet által nyújtott szolgáltatásokat igénybe vevők tájékoztatását az azokat potenciálisan érintő kiberfenyegetésről vagy az ilyen fenyegetés elhárításához szükséges megelőző intézkedések várható hatásairól.

25. §

A törvényjavaslat megállapítja az érintett szervezet által fizetendő éves kiberbiztonsági felügyeleti maximális mértékét, továbbá különös szabályokat rögzít arra az esetre, ha az érintett szervezet a polgári törvénykönyvről szóló törvény szerinti elismert vagy tényleges vállalatcsoportba tartozik, vagy egy konszolidációs körbe tartozó vállalkozáscsoportban vesz részt. A kiberbiztonsági felügyeleti díj mértéke az előző üzleti évi nettó árbevételre vetítve százalékosan, továbbá maximális, összegszerű korláttal kerül meghatározásra.

26. §

A törvényjavaslat a hatóság eljárására vonatkozó adminisztratív rendelkezéseket tartalmazza, valamint a hatóság által az érintett szervezetekről vezetett nyilvántartás részletszabályait határozza

meg. Rögzíti továbbá az érintett szervezet kiberbiztonsági audit kötelezettsége kapcsán az auditorral való szerződéskötés és első kiberbiztonsági audit lefolytatásának határidejét.

27. §

A törvényjavaslat meghatározza a biztonsági események bejelentési kötelezettségét a kijelölt szervezet felé, valamint rögzíti, hogy a biztonsági események kezelését a külön jogszabályban foglaltak szerint kell elvégezni. Biztonsági eseménykezelésbe közreműködő bevonása esetén a közreműködőnek a hatóság által kiállított tanúsítvánnyal kell rendelkeznie.

A törvényjavaslat szerinti bejelentési kötelezettség nem érinti a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) szerinti jelentési kötelezettséget.

28. §

Felhatalmazó rendelkezések.

29. §

Hatályba léptető rendelkezések.

30. §

Átmeneti rendelkezések.

31. §

Az Alaptörvény sarkalatosságra vonatkozó követelményének való megfelelés.

32. §

A törvényjavaslat az Európai Unió jogának való megfelelésről rendelkezik.

33-38. §

Egyes érintett törvények módosítása a törvényjavaslattal való összhang biztosítása érdekében.

39-51. §

Módosító rendelkezések a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény új feladatokkal történő kiegészítése érdekében.